CLAIMS

What is Claimed is:

1. A computer-implemented method for protecting a host network from a flood-type denial of service attack, comprising the steps of:

passively collecting a data packet from data received by the host network, the data packet comprising information indicating the attack;

comparing the information in the data packet to a signature of an attack type of the attack to determine whether the information and the signature comprise matching data; and

detecting the attack in response to a determination that the signature and the information comprise matching data.

2. The method according to Claim 1, further comprising the step of providing a pathway for an offensive countermeasure against a source of the attack.

3. The method according to Claim 1, further comprising the step of generating the signature for the attack type of the attack.

4. The method according to Claim 3, wherein the attack type comprises a plurality of data packets, and

wherein said generating step comprises the steps of:

identifying a repetitive pattern in the plurality of data packets of the attack type; and

storing the repetitive pattern as the signature of the attack type.

5. The method according to Claim 3, wherein the information comprises information from a header of the data packet, and

wherein said comparing step comprises comparing the information from the header to the signature.

6. The method according to Claim 3, wherein the signature comprises a repetitive pattern of information from data packets of the attack type.

7. The method according to Claim 6, wherein the repetitive pattern comprises information included in a header of each data packet of the attack type.

8. The method according to Claim 1, further comprising the step of initiating a defensive countermeasure to protect the host network from the attack in response to detection of the attack.

9. The method according to Claim 8, further comprising the step of confirming the attack before initiating the defensive countermeasure to protect the host network from the attack.

10. The method according to Claim 9, wherein said confirming step comprises the steps of:

setting a load threshold for the host network;

determining the current load on the host network;

determining whether the current load exceeds the load threshold; and

confirming the attack in response to a determination that the current load exceeds the load threshold.

11. The method according to Claim 8, further comprising the step of tracing a route of the attack to determine whether a single source produced the attack,

wherein said initiating step comprises initiating a single-source, defensive countermeasure in response to a determination that a single source produced the attack, and

wherein said initiating step comprises initiating a multiple-source, defensive countermeasure in response to a determination that a single source did not produce the attack.

12. The method according to Claim 11, wherein said collecting step comprises collecting a plurality of data packets from data received by the host network,

wherein said tracing step comprises comparing information in each of the data packets to determine if the information in each data packet is the same, and

wherein said tracing step determines that a single source produced the attack in response to a determination that the information in each data packet is the same.

13. The method according to Claim 12, wherein the information in each data packet comprises a source IP address.

14. A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 1.

15. A computer-implemented method for protecting a host network from attack, comprising the steps of:

passively collecting a plurality of data packets from data received by the host network;

comparing information in respective data packets to determine if any pair of the data packets comprise similar information; and

detecting the attack in response to a determination that the pair of data packets comprise similar information.

16. The method according to Claim 15, further comprising the step of providing a pathway for an offensive countermeasure against a source of the attack.

17. The method according to Claim 15, wherein said comparing step comprises comparing information in the respective data packets to determine if about forty percent of the data packets comprise similar information, and

wherein said detecting step detects the attack in response to a determination that about forty percent of the data packets comprise similar information.

18. The method according to Claim 15, wherein the information in the respective data packets comprises a header, and

wherein said comparing step comprises comparing the headers of the respective data packets.

19. The method according to Claim 15, further comprising the steps of:

setting a load threshold for the host network;

determining the current load on the host network;

comparing the current load to the load threshold; and

confirming the attack when the current load exceeds the load threshold.

20. The method according to Claim 15, further comprising the steps of:

determining whether the attack comprises a new attack type; and

learning a new signature of the new attack type in response to a determination that the attack comprises a new attack type.

21. The method according to Claim 20, wherein said learning step comprises the steps of:

identifying a repetitive pattern in data from the plurality of data packets of the attack; and

storing the repetitive pattern as the new signature of the new attack type.

22. The method according to Claim 21, wherein the data from the plurality of data packets comprises a header for each respective data packet, and

wherein said identifying step comprises identifying a repetitive pattern in the headers of the plurality of data packets of the new attack type.

23. The method according to Claim 15, further comprising the step of initiating a defensive countermeasure to protect the host network from the attack in response to detection of the attack.

24. The method according to Claim 23, further comprising the step of tracing a route of the attack to determine whether a single source produced the attack,

wherein said initiating step comprises initiating a single-source, defensive countermeasure in response to a determination that a single source produced the attack, and

wherein said initiating step comprises initiating a multiple-source, defensive countermeasure in response to a determination that a single source did not produce the attack.

25. The method according to Claim 24, wherein said tracing step comprises comparing a source IP address in each of the data packets to determine if the source IP address in each data packet is the same, and

wherein said tracing step determines that a single source produced the attack in response to a determination that the information in each data packet is the same.

26. A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 15.

27. A computer-implemented method for protecting a host network from attack, comprising the steps of:

detecting the attack based on a load capacity of the host network; and

initiating a defensive countermeasure to protect the host network from the attack in response to detection of the attack.

28. The method according to Claim 27, wherein said detecting step comprises the steps of:

setting a load threshold for the host network, the load threshold establishing an amount of the load capacity beyond which the attack is indicated;

determining the current load on the host network; and

comparing the current load to the load threshold,

wherein said detecting step detects the attack when the current load exceeds the load threshold.

29. A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 27.

30. A computer-implemented method for generating a signature of a network attack type, the attack type corresponding to a flood-type denial of service attack comprising a plurality of data packets, said method comprising the steps of:

examining information included in each of the plurality of data packets;

identifying a repetitive pattern in the information of at least two of the plurality of data packets; and

storing the repetitive pattern as a signature of the attack type.

31. The method according to Claim 30, wherein the information comprises a header.

32. A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 30.

33. A computer-implemented method for countering a flood-type denial of service network attack from a single source, the attack comprising an attacking data packet and the network comprising a host router, said method comprising the steps of:

reading an attacking source IP address from the attacking data packet; and

preventing an incoming data packet comprising the attacking source IP address from entering the host network through the host router.

34. The method according to Claim 33, wherein said preventing step comprises the steps of:

determining whether the incoming data packet comprises the attacking source IP address;

rejecting the incoming data packet in response to a determination that the incoming data packet comprises the attacking source IP address; and

accepting the incoming data packet in response to a determination that the incoming data packet does not comprise the attacking source IP address.

35. The method according to Claim 34, further comprising the step of writing the attacking source IP address to an access control list of the host router, the access control list identifying a source from which the host router will reject a data packet,

wherein said determining step comprises determining whether the access control list comprises the source IP address of the incoming data packet.

36. The method according to Claim 35, further comprising the step of storing the attacking source IP address in an access control file,

wherein said writing step comprises writing the contents of the access control file to the access control list of the host router.

37. The method according to Claim 36, further comprising the steps of:

detecting a revised version of the access control file; and

updating the access control list of the host router to correspond to the revised access control file in response to detecting the revised access control file.

38. The method according to Claim 35, further comprising the step of applying the access control list to an incoming interface of the host router.

39. The method according to Claim 33, further comprising the steps of:

storing a block time for the attacking source IP address, the block time indicating a time period during which said preventing step is performed;

determining whether the block time has expired; and

discontinuing said preventing step in response to a determination that the block time has expired.

40. The method according to Claim 35, further comprising the steps of:

storing a block time for the attacking source IP address, the block time indicating a time period during which said preventing step is performed;

determining whether the block time has expired; and

removing the attacking source IP address from the access control list of the host router in response to a determination that the block time has expired.

41. A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 33.

42. A computer-implemented method for countering a flood-type denial of service network attack from multiple sources, the attack comprising a plurality of attacking data packets and the network comprising a host router, said method comprising the steps of:

reading an attack target IP address from one of the plurality of attacking data packets; and

preventing an incoming data packet having the attack target IP address from entering the host network through the host router.

43. The method according to Claim 42, wherein said preventing step comprises the step of sending the incoming data packet having the attack target IP address to a null interface of the host router.

44. The method according to Claim 42, further comprising the steps of:

determining whether the incoming data packet comprises the attack target IP address;

accepting the incoming data packet in response to a determination that the incoming data packet does not comprise the attack target IP address; and

sending the incoming data packet to a null interface of the host router in response to a determination that the incoming data packet comprises the attack target IP address.

45. The method according to Claim 44, further comprising the step of automatically updating an upstream router coupled to the host router to direct a data packet destined for the attack target IP address to a null interface of the upstream router.

46. The method according to Claim 44, further comprising the step of writing the target IP address to a null route list of the host router, the null route list identifying a target IP address for which a data packet will be sent to the null interface of the host router,

wherein said determining step comprises the step of comparing the target IP address of the incoming data packet to the null route list to determine whether the incoming data packet comprises the attack target IP address.

47. The method according to Claim 46, further comprising the step of storing the attacking source IP address in a null route file,

wherein said writing step comprises writing the contents of the null route file to the null route list of the host router.

48. The method according to Claim 47, further comprising the steps of:

detecting a revised version of the null route file; and

updating the null route list of the host router to correspond to the revised null route file in response to detecting the revised null route file.

49. The method according to Claim 42, further comprising the steps of:

storing a block time for the attack target IP address, the block time indicating a time period during which said preventing step is performed;

determining whether the block time has expired; and

discontinuing said preventing step in response to a determination that the block time has expired.

50. The method according to Claim 46, further comprising the steps of:

storing a block time for the attack target IP address, the block time indicating a time period during which said preventing step is performed;

determining whether the block time has expired; and

removing the attack target IP address from the null route list of the host router in response to a determination that the block time has expired.

51. A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 42.

52. A system for protecting a host network from a flood-type denial of service attack, the host network comprising a host router, said system comprising:

an interface, coupled to the host router, operable for communicating data packets to and from the host router;

a database operable for storing a signature for an attack type of the attack, the attack type comprising a plurality of data packets;

a packet sniffing module operable for collecting a data packet from data received by the host router, the data packet comprising information indicating the attack; and

a decision module operable for detecting the attack by determining whether the information in the data packet matches the signature stored in the database.

53. The system according to Claim 52, wherein said countermeasure module is further operable for providing a pathway for an offensive countermeasure against a source of the attack.

54. The system according to Claim 52, further comprising a self-learning module operable for generating the signature by identifying a repetitive pattern in the plurality of data packets of the attack type.

55. The system according to Claim 52, wherein the information in the data packet comprises information from a header of the data packet.

56. The system according to Claim 52, wherein the signature comprises a repetitive pattern of information in the plurality of data packets of the attack type.

57. The system according to Claim 56, wherein the repetitive pattern comprises information included in a header of each data packet of the attack type.

58. The system according to Claim 52, wherein said decision module is further operable for confirming the attack before said countermeasure module initiates the defensive countermeasure.

59. The system according to Claim 58, wherein said decision module is operable for confirming the attack by determining whether a current network load exceeds a specified load threshold, and

wherein the decision module confirms the attack in response to a determination that the current network load exceeds the specified load threshold.

60. The system according to Claim 52, further comprising a countermeasure module operable for initiating a defensive countermeasure to protect the host network from the attack in response to the decision module detecting the attack.

61. The system according to Claim 60, further comprising a trace route module operable for tracing a route of the attack to determine whether a single source produced the attack,

wherein said countermeasure module is further operable for initiating a single-source, defensive countermeasure in response to a determination that a single source produced the attack and for initiating a multiple-source, defensive countermeasure in response to a determination that a single source did not produce the attack.

62. The system according to Claim 61, further comprising a router daemon module operable for automatically running said trace route module for tracing the route and said countermeasure module for initiating the defensive countermeasure.

63. The system according to Claim 61, wherein said packet sniffing module is further operable for collecting a plurality of data packets from data received by the host router, and

wherein said trace route module is further operable for determining that a single source produced the attack by determining whether a source IP address in each data packet is the same.

64. A system for protecting a host network from a flood-type denial of service attack, the host network comprising a host router, said system comprising:

an interface, coupled to the host router, operable for communicating data packets to and from the host router;

a packet sniffing module operable for collecting a plurality of data packets from data received by the host router; and

a decision module operable for detecting the attack by comparing information in respective data packets to determine if any pair of data packets comprise similar information.

65. The system according to Claim 64, further comprising a countermeasure module operable for initiating a defensive countermeasure to protect the host network from the attack in response to detection of the attack.

66. The system according to Claim 64, wherein the information in the respective data packets comprises information of a header in the respective data packets.

67. The system according to Claim 64, wherein said decision module is further operable for confirming the attack by determining whether a current network load exceeds a specified load threshold, and

wherein the decision module confirms the attack in response to a determination that the current network load exceeds the specified load threshold.

68. The system according to Claim 64, further comprising a self-learning module operable for determining whether the attack comprises a new attack type and for learning a new signature of the new attack type in response to a determination that the attack comprises a new attack type.

69. The system according to Claim 68, further comprising a database, wherein said learning module is further operable for identifying a repetitive pattern in data from the plurality of data packets of the attack and for storing the repetitive pattern in the database as the new signature of the new attack type.

70. The system according to Claim 69, wherein the data from the plurality of data packets comprises information in a header of each respective data packet.